Safety Tips for using Public WiFi Cheat Sheet

by [deleted] via cheatography.com/2754/cs/6669/

Introduction

With the number of public Wi-Fi networks increasing and the number of mobile data transfers keeping pace, the use of public Wi-Fi is a significant and growing security risk. As the number of hotspots and mobile users continue to expand, attacks will increasingly compromise email accounts, passwords, Social Security numbers, and credit cardholder data. Hackers will eavesdrop on communications, steal corporate information, gain access to banking accounts, and infect IT systems with malware.
What precautions can users take to help secure their use of public Wi-Fi networks? Here are five tips for using these networks safely.

Credits: Dirk Gates is executive chairman and founder of Xirrus http://www.infoworld.com/article/3007288/network-security/5-tips-for--using-public-wi-fi-securely.html?phint=newt%3Dinfoworld_mobile_-rpt&phint=idg_eid%3D63faf60c70c3592e8cb9eed1a2f958d8#tk.IFW-NLE_nlt_mobilehdwr_2015-11-30

Verify the network

Before going online, verify that the network is the provider's official system. Don't assume the strongest signal is coming from the trusted network. If there's any doubt about the proper SSID, ask. This helps prevent a man-in-the-middle attack, where a rogue access point may capture everything the user does. Sometimes scammers even demand a fake fee for access, thus acquiring both credit card information and a payment.

The safest way to "verify" a network is to establish a secure VPN back to a known location (such as an office or a home) and tunnel all your traffic through it. If the VPN tunnel can be established, then you're likely on a safe network.
https://technet.microsoft.com/en-us/library/ff687730%28v=ws.10%-29.aspx
https://www.kentlaw.iit.edu/Documents/Departments/CLC/Wireless%-20Instructions/VerifyWirelessNetworkName.pdf

Implement a VPN

A common action is to implement a VPN capability. The VPN establishes an encrypted tunnel through which they can access company information, but also surf the Internet and engage in personal business.** VPN offers a series of controls to protect both the system and its traffic, but requires a VPN application on each device to encrypt the connection from end to end.
Because of its inconvenience, many users continue to check Facebook, read the news, and carry out their other personal Internet business without going through the VPN. This is a mistake. As long as they are online, users are exposing their device to hackers on the public Wi-Fi network. If a hacker can get into a machine, they can see every sensitive file, even if it is not open at the time.

WiFi Security Breach

Avoid Logging in

When on a public network, ideally browse only websites that do not require login credentials. **However, if you need to log in -- for example, to access personal email -- it is best to go to websites that support the HTTPS protocol,** which encrypts the communications between website and browser. Note that images may still be distributed via HTTP since links are not typically encrypted.

Use two-factor authentication

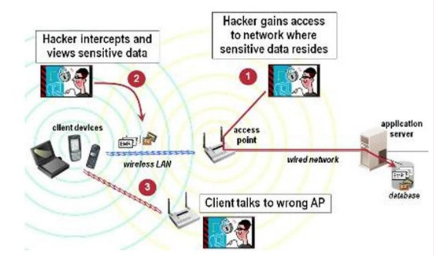
Two-factor authentication identifies users with a two-step process, combining components from the system and a knowledge factor provided by the user. With these extra steps (which take only a few seconds), most illicit actors can be blocked from the system. If accessing company email and other systems requires two factors, even if a bad guy sniffs a user's password, the password alone won't provide access to the company system.

https://en.wikipedia.org/wiki/Two-factor_authentication

Beware Open SSID

One of the hidden challenges of mobile networks is that once a device has joined a specific network, it will jump back onto that network whenever the user is within range. To prevent this, users should turn off network discovery options like "Remember networks this computer has joined," or get into the habit of deleting the network's SSID profile after each session. This way, users can't be coaxed into accidentally accessing a network with a similar name. For example, an iPhone will automatically hop onto any network called "AT&T." Similarly, many notebooks are set up to advertise their internal SSIDs -- which is why you can walk down a hotel hall and see the hard drive in every room..

It's important keep mobile devices from blindly hopping on networks advertising those SSIDs -- and to stop advertising their own SSIDs. **Whenever a device is used on a public network, sharing should be Off and the firewall On.**
http://windows.microsoft.com/en-US/windows-8/turn-sharing-on-or-off



Hacker is the Man in the Middle